

ABSTRACT

A method for providing a proactive security in proactive operating environment. The proactive operating environment includes a group of proactive servers communicating over a network. Each proactive server (PS_i) includes a storage that includes a non erasable part that stores a public, non proactive related, key V_{Start}^I . The storage further includes an erasable part for storing private and public data. The proactive server has a discardable one-time private key S_{Start}^I that corresponds to the public key V_{Start}^I . The proactive server further has configuration data C . There is further provided a processor for providing a proactive services to applications. The proactive server has a group public proactive key V_{CERT} , common to the group of proactive servers and a share S_{CERT}^I of a corresponding private proactive key S_{CERT} . The method further includes the steps of invoking initialization procedure for generating restore related information, and invoking a restore procedure for utilizing the public, non proactive related, key V_{Start}^I and the restore related information for restoring the public proactive key V_{CERT} .